Section V:	**Physical Security**
Title:	**Physical Access Control Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**May 16, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To define physical safeguards to be employed by Divisions and Offices of the North Carolina (NC) Department of Health and Human Services (DHHS) for controlling access to a facility for the protection of all elements of Information Technology (IT) assets relating to their use and operation.

STANDARD

Background

Controlling physical access to IT assets is an important element in protecting the availability and integrity of services provided by the assets. Many considerations factor into the selection and implementation of physical access controls. Using multiple layered controls such as deterrence and detection safeguards and response and recovery plans provide the greatest span of asset protection.

2.0 Physical Access Control Considerations

Different types of assets may require specific access control systems to be able to effectively limit access to authorized personnel. Since information systems are comprised of various components, the availability of the information system as a whole is one of the main goals of an effective access control. The availability of the entire information system is only as strong as the weakest control afforded each component.

Compliance with the Occupational Safety and Health Administration (OSHA), Americans with Disabilities Act (ADA), and other state and federal safety codes must always be addressed when selecting and implementing access controls. Special circumstances such as cleaning staff, maintenance, and service personnel access must also be considered as they may require exceptions or alternate procedures.

2.1 Assets That Require Access Controlled Protection

An inventory of assets controlled by the Division or Office should be maintained as a part of the access control plan for the organization. The following is a partial list of assets that require implementation of access control protections:

- Network devices, electronic media, databases, servers, and computing equipment
- Power lines, control and distribution panels, switches, and communication equipment
- HVAC and other environmental controls

2.2 Physical Access Control Related Elements

Effective physical access control systems depend on principles and procedures in addition to the actual physical control system employed. The following elements must be considered to ensure the performance of the access control system:

- Access authorization policies shall be based on a valid need to know and/or need to use
- The person that performs the access authorization shall not be allowed to grant themselves access
- Periodic review of the access list ensures all authorizations are current and appropriate
- Employee termination and/or job duty changes effecting access shall be updated on all access lists
- Training shall be delivered to all workforce members as necessary
- Document the response and recovery to an access control breech to assist in any necessary modification of the control in the future

2.3 Access Control Performance Assurance

Performance of an access control system shall be periodically reviewed to ensure that the intended protection is being realized. The following list represents activities that need to be performed as appropriate:

- Periodic review of access logs provides verification that the access control system is working properly
- Compare access logs with authorization lists to detect unauthorized access events
- If implemented, review key control procedures to ensure access has not been compromised
- Compare authorization list changes with access change requests to detect the potential for unauthorized access
- Develop and implement a corrective action plan for any asset control measure found to be faulty or ineffective

2.4 Responsibility for Physical Access Controls

Management must assign physical access control responsibilities to a primary point of contact (POC). A second workforce member will be designated as an 'alternate' POC to the primary. Both the primary and secondary POC should be knowledgeable about physical access controls and the importance to the Division or Office.

2.5 Maintenance and Testing of Physical Access Controls

Both the primary and secondary POC are responsible for ensuring that physical access controls are working as intended and must ensure that regular maintenance is performed as required. Physical access testing, both perimeter and internal, shall be performed on a periodic basis (recommend every three months).

3.0 Safeguards

3.1 General Safeguards

The following are recommended general safeguards that should be implemented to help protect assets:

- The NC DHHS Security Standards, Physical Security - Identification & Visitor Control Standard must be implemented
- Access control logs must be used for all areas that require a high degree of protection
- An audit trail of all individuals who have access to areas that contain critical assets shall be maintained
- Off-site storage facilities shall be afforded the same level of protection as a main processing site

3.2 Controlled Area Access Safeguards

The following are safeguards for access to controlled areas that shall be implemented, if appropriate:

- Access to controlled areas should require positive identification by either an automated photo badge system, mechanical device such as cipher or key locks, or coverage by staff at entrances to provide adequate protection
- All keys and badges must be recovered and applicable entry codes changed within one day when workforce members terminate or transfer employment
- Access badges shall be programmed to allow entry into assigned facilities only
- Controlled areas should maintain a low profile with no obvious indication of its purpose
- Limit ingress and egress route vulnerabilities
- Doors, locks, bolts, hinges, frames, and other building apparatuses must be constructed to reduce the probability of unauthorized entry
- Restrict controlled area entrances while ensuring adequate emergency exits
- Employ video cameras or intrusion detection systems as appropriate to asset value and threat level
- Employ a double door man trap system as appropriate to asset value and threat level
- Equip all perimeter fire doors with alarms as well as devices that close and lock the doors automatically
- Controlled areas should use true floor-to-ceiling walls of adequate sound and penetration protection

3.3 Cabling Safeguards

Divisions and Offices installing or maintaining telecommunication and/or power cabling should consider the following practices to increase the security and physical protection of the cabling:

- Use underground cabling, where possible, or provide lines with adequate alternative protection
- Run network cabling through overhead cable troughs, pipes, or similar conduits
- Power and communication cables shall be segregated

3.4 Protective Container Safeguards

Facilities and areas used for storing equipment and media containing confidential data shall be controlled and all cabinets fitted with locking devices sufficient to protect the equipment or media from unauthorized access. When a safe is used, the location of the safe shall be inconspicuous so as not to draw unnecessary attention to the safe, and must be in an area that is subject to regular surveillance. Access shall be limited to authorized personnel who require access to perform their job duties.

4.0 Special Considerations for Key Lock Systems

When a key lock entry control system is employed, various elements must be addressed to assure satisfactory performance. The following are some of the considerations:

- Each key must contain a unique identification number that is recorded in a key assignment register
- All keys assigned to workforce members must be recorded in a key assignment register
- When loss or compromise of a key is suspected, lock changes must be accomplished in as timely a manner as possible
- "Do not duplicate" key marking must be placed on every key

Procedures that protect and limit access to master key(s) must be established and documented.

Reference:

- HIPAA Administration Simplification - Act 45 C.F.R. Part 160 and 164.
  - HIPAA - 45 C.F.R. § 164.310 (a)(1) Standard: Facility access controls.
  - HIPAA - 45 C.F.R. § 164.310 (a)(2) Implementation specifications: (i) Contingency operations.
  - HIPAA - 45 C.F.R. § 164.310 (a)(2) Implementation specifications: (ii) Facility security plan.
  - HIPAA - 45 C.F.R. § 164.310 (a)(2) Implementation specifications: (iii) Access control and validation procedures (iv) Maintenance records.
  - HIPAA - 45 C.F.R. § 164.310(c) Standard: Workstation Security.

- NC Statewide Information Security Manual, Version No. 01
  - Chapter 2 - Controlling Access to Information and Systems, Section 01: Controlling Access to Information and Systems
    - Standard 020107 - Securing Against Unauthorized Physical Access
    - Standard 020113 - Types of Access Granted to Third Parties
    - Standard 020119 - Diagnostic and Configuration Port Controls
  - Chapter 3 - Processing Information and Documents, Section 02: System Operation and Administration
    - Standard 030203 - Controlling Data Distribution
    - Standard 030206 - Managing System Operations and System Administration
    - Standard 030215 - Commissioning Facilities Management for Information Technology

- Chapter 3 - Processing Information and Documents, Section 06: Backup, Recovery and Archiving
  - Standard 030602 - Backing Up Data on Portable Computers
- Chapter 5 - Securing Software, Peripherals and Other Equipment, Section 01: Purchasing and Installing Hardware
  - Standard 050103 - Installing New Hardware
- Chapter 5 - Securing Software, Peripherals and Other Equipment, Section 02: Cabling, UPS, Printers and Modems
  - Standard 050206 -Installing and Maintaining Network Cabling
- Chapter 5 - Securing Software, Peripherals and Other Equipment, Section 03: Consumables
  - Standard 050302 - Using Removable Storage Media, Including Diskettes and CDs, Standard
- Chapter 5 - Securing Software, Peripherals and Other Equipment, Section 05: Using Secure Storage
  - Standard 050501 - Using Lockable Storage Cupboards
  - Standard 050502 - Using Lockable Filing Cabinets
  - Standard 050504 - Using a Safe
- Chapter 6 - Combating Cyber Crime, Section 01: Combating Cyber Crime
  - Standard 060104 - Defending Against Premeditated Internal Attacks
- Chapter 8 - Developing and Maintaining In-House Software, Section 05: Other Software Development
  - Standard 080501 - Acquiring Vendor Developed Software
- Chapter 9 - Dealing with Premises Related Considerations, Section 01: Premises Security
  - Standard 090101 - Preparing Premises to Site Computers and Data Centers
  - Standard 090102 - Securing Physical Protection of Computer Premises
  - Standard 090104 - Physical Access Control to Secure Areas
  - Standard 090105 - Challenging Strangers on Agency Premises
- Chapter 9 - Dealing with Premises Related Considerations, Section 02: Data Stores
  - Standard 090201 - Managing On-Site Data Stores
  - Standard 090202 - Managing Remote Data Stores
- Chapter 9 - Dealing with Premises Related Considerations, Section 03: Other Premises Issues
  - Standard 090301 - Electronic Eavesdropping
  - Standard 090302 - Cabling Security

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual
  - Acceptable Use for DHHS Information Systems Policy
  - Data Protection Policy
  - ITS Operations Security Policy
  - Network and Telecommunications Security Policy
  - Physical and Environmental Security Policy
  - Security Testing Policy
  - Wireless Security Policy